ISSN. 1363-6650

FEBRUARY 1997
Issue 2

International Journal of FORENSIC COMPUTING™

Contents

International Journal of Forensic Computing
Third Floor, Colonnade House
High Street, Worthing, West Sussex
UK BN11 1NZ
Tel: +44 (0) 1903 209226
Fax: +44 (0) 1903 233545
e-mail: ijfc@pavilion.co.uk
http: //www.forensic-computing.com

When Experts Disagree

This Journal has been devised with the aim of providing a platform for informed discussion and a regular source of intelligence about the use and presentation of computer based material in courts of law. Many of the principles involved are either self-evident or borrowed from similar forensic disciplines in other areas. Where they apply, these principles have been imported to help build the cornerstone of a new science but there are naturally some areas which have a greater relevance and carry much more weight when dealing with computers.

One of the major positive aspects of forensic computing is that machine content and operation may often be demonstrated retrospectively with absolute accuracy. Thus the effects of malicious code may be proven beyond doubt - and cause and effect can be illustrated without the need for the courts becoming involved in the complexities of computer operation. However, these very complexities can result in perfectly valid evidence being rejected as inadmissible, particularly when experts disagree.

The level of expertise possessed by any individual has always been difficult to quantify, particularly where legal requirements are concerned. It also appears that a significant proportion of people with a little technical knowledge of computers have used that knowledge in criminal or at least questionable activities. Some of these individuals, perceiving that there may be money to be made from their expertise, have offered their 'expert' services to the legal profession. There may be reservations about the integrity of some of these 'Poachers turned Gamekeepers' and when these are considered alongside the human need to demonstrate superior knowledge, a conflict can arise between the need for absolute proof and the complexities which may be introduced to confirm or deny it.

It is vital that the integrity of the evidence and the accuracy of the investigations are unimpeachable. However, investigating the intricacies of computer operation to a standard acceptable by a court of law can be a lengthy and expensive process in which the time and cost will increase dramatically if extra work is needed to confirm or deny additional complexities. There is no doubt that this can become an important factor when planning the presentation of a case. It might therefore be deemed necessary to draw attention to gratuitous elaborations by the expert on either side, particularly if there is a history of misuse of expertise.

The notion of 'reasonable doubt' has long been a cornerstone of English Criminal Law and most people accept it as a proper protection against potential injustice. It is a principle conceived to safeguard a defendant against conviction on evidence which is flimsy or inconclusive. However, it must also be remembered that injustice also occurs when the guilty go free. There has been much recent debate about the efficacy of the jury system when considering extremely complex fraud cases and it seems that the arguments advanced both for and against this system might also be applied in cases where the complexities of computer evidence are involved. It is to be hoped that the pages of this Journal might carry informed observations and opinions in such a debate as it affects computer based evidence. ■

Overview

Internet Banking

According to some, cyber-criminals are rubbing their hands at the prospect of a boom in Internet banking. The scenario is that hackers, fraudsters and electronic highwaymen will plunder accounts using little more than a PC and a modem. But is all this wild exaggeration, or are criminal investigators going to have to contend with a new breed of bank robber?

Around 50 million people have access to the Internet, and this number is expected to reach 200 million by 1998. It is the vast number of people hooked up to the Internet, coupled with the ability to offer a 24-hour service with no geographical boundaries, that is attracting many banks and financial institutions to this giant computer network. So is the prospect of reducing operational costs.

But one issue making many banks nervous about using it is security: "There's no doubt that this is making banks very cautious," says Daryl Booth, head of delivery channel development at the UK clearing bank Barclays. As a result, few banks are currently prepared to offer online banking services.

A survey by Booz•Allen found that although over 600 banks had sites on the Internet, only two per cent of European banks and one per cent of US banks offered full banking services over it. Some banks have opted for privately-owned online services, such as CompuServe, rather than the Internet.

But the Security First Network Bank (SFNB), based in Atlanta, USA, offers full Internet banking to over 2000 customers. The SFNB uses a number of security features, which include issuing each customer with a PIN code, and encrypting any data that is sent over the Internet. The bank's internal computer network is protected by a 'firewall', which filters all electronic traffic.

This is an impressive array of weapons, but you can be sure that hackers will be looking for vulnerable spots in any Internet banking system.

Some believe that Internet banking will explode when there is widespread use of a technology known as public key cryptology. The key - a complex mathematical number - is divided into two parts, a public key and a private key. The public key is available to anyone, and may be printed in a directory or even posted on to the Internet. The private key is kept secret by the owner and used for decryption. The public key system also makes it possible to produce a 'digital signature'. This is created by the sender, who encrypts part of the message with his or her private key. The recipient of the message uses the sender's public key to decrypt the segment and thus confirm the identity of the sender. "This is important, because a bank will need to be confident that it is communicating with the genuine customer, and the customer needs to be certain that he's dealing with his bank," says Michael McConnell, vice-president of Booz•Allen.

Another weapon will be an audit trail that allows a bank to follow a transaction from the customer's PC to the host server, but as Booth points out, this is a demanding process: "You've got to follow something which goes from a PC on to a public switched telephone network and then through a variety of pathways through the Internet."

One problem is the attitude of governments towards public key technology. The potential for criminals such as terrorists, drug smugglers and money launderers to use powerful encryption systems to conceal their operations has led various governments to pass laws restricting the use of the technology. In France, for example, it is illegal to manufacture, import or use encryption systems without government permission.

The US classes encryption systems as munitions and tightly controls their export. Barclays Bank spent months negotiating with the US National Security Agency to obtain permission to use a 64-bit key (developed by the encryption company RSA) for a trial online service called PurchaseOnline. But if Internet Banking is to take off - and be secure - public key systems will need to be both powerful, and widely available. ■

by **George Cole**
Computer Consultant & Technical Journalist

Forensic Principles

The Fundamentals of Computer Forensics (part 2)

Forensic Considerations

Information stored on computer equipment can be considered from a number of different viewpoints:- at one level we may have varying patterns of magnetism written to a special surface coating whilst higher up the hierarchy *the same information* may appear as intelligible text gained by considering the same patterns translated according to accepted computing standards.

Although it will usually be possible to examine the contents of a computer directly, the risk of contamination and the fact that such contamination may be impossible to detect means that direct examination should be avoided wherever possible.

From the discussion of media independence *(see Issue 1)* it will be noted that for all practical purposes an exact and indistinguishable copy can be made of the permanent, semi-permanent and volatile source information. To reduce complexity and the risk of error in additional processing subsystems, the copy process should be designed for forensic use with due regard to the need for hygiene and accuracy, and should ideally be managed by the processor and storage subsystem of the device being copied. The only additional peripherals being the device where the copy is to be stored and its associated interface. This is not always possible and it may be necessary to relocate the storage system under investigation to an alternative hardware installation to complete the copy. Note that even under these circumstances there will only be one processor involved in the transfer of information. Such a copy process may be described as forensically sound.

I define the forensic examination process as consisting of three distinct phases: collection, examination and evaluation. These must be undertaken in this order with examination and evaluation taking place upon the copied information.

This immensely powerful capability of being able to conduct investigations on forensically sound copies of the data rather than on the data itself preserves the integrity of the original information as best evidence. Couple this with the fact that by far the largest proportion of investigations are concerned with the overall content of files which require few or no subjective opinions, and it will be seen that once a forensically sound copy has been made, investigation can often be completed quite adequately by operatives with a limited degree of computer expertise.

For a full investigation it is vital that the information collection process must be undertaken in a completely non-discriminatory manner. That is to say that the pattern of stored information must be collected without regard to its relationship to anything other than itself and its associated hardware. For example, the contents of a 500 megabyte fixed magnetic disk should be copied sector by sector from sector 0 to the end without regard to the content - even if only 50 megabytes are configured as currently in use. In this manner any data which might be hidden from or inaccessible to the resident operating system will be copied and available for examination. This does not disqualify information copied solely on the basis of the current operating configuration but it does ensure the completeness of the copy and may provide additional evidence in confirmation or rebuttal.

It is also best to copy everything so that changes in requirements dictated by the progress of an ongoing investigation can be accommodated. Thus although the exigencies of a particular case may indicate that only

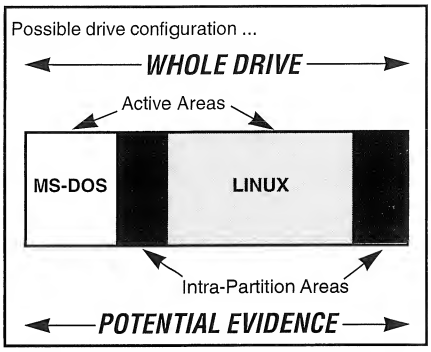


Figure 1: The whole drive must be considered as potential evidence, not just the active areas.

active file information is required, subsequent discovery of encrypted, protected or deleted files would not necessitate re-copying of the original data. For similar reasons of completeness, a copy of the ROM and CMOS contents is desirable in case they are required for correct interpretation of the semi-permanent information.

Where computer stored information has been copied using commercial file transfer facilities it must be accepted that such copies are incomplete and this might provide justification for the evidence thus gained to be declared invalid on the grounds that unexamined data within active storage might have confirmed or denied a relevant submission. For example if a number of pornographic image files were discovered in semi-permanent computer storage, this might appear to confirm a charge of possession of pornography. However, if the defence submission was that these files had been placed there by someone other than the defendant and from floppy disks rather than communications access, only a complete copy of the relevant computer system (including deleted and unallocated space) would be able to confirm or deny such a submission. If reference to the original computer (in its original state) were also not possible then the defence would be denied the opportunity of proving their submission.

Considerations for the Courts

Since 'presentation in a court of law' is the end of any forensic computing work, the considerations for the courts and their ▶

standards of accepting evidence must be a priority for any forensic investigator.

My own experience has been mainly concerned with assisting the police in prosecuting criminal cases in the UK. The following discussion reflects that bias, but the principles can equally be applied to defence and civil matters both in the UK and overseas.

The presentation of observations and conclusions in a court entails maintaining the absolute integrity of the evidence under examination. Less obvious is the vital requirement of maintaining evidential continuity.

The concept of media independence illustrates that information might be altered without trace. This makes it paramount that a forensically sound copy is taken as quickly as possible when a computer is seized for examination so that the computer may then be placed in secure storage. Thus the opportunity for tampering with the contents is reduced to a minimum. Thereafter all reports, observations and/or conclusions should be derived from the copied information with the overriding proviso that their accuracy can be demonstrated in open court upon the original computer.

Occasions have arisen in the UK where the owner of the computer quite legitimately claims that if he is deprived of the computer his business will suffer (or even fail). Under these circumstances, it is suggested that a forensically sound copy will be an adequate substitute for the original computer as best evidence. However, consider the possibility that a single copy is taken of a computer, which is then returned to the owner. The owner subsequently erases all trace of any incriminating files and then claims that these files were introduced to the copy during forensic examination and never existed on the original computer. The courts might be unable to determine the truth of the matter from the evidence of a single copy. Consider also the situation where a computer has been seized and copied but the defence require access to it for their own purposes. If the defence access is not supervised by someone at least as knowledgeable there is the possibility that information could be changed or erased (again without trace). This would also leave the courts unable to determine which is the true evidence.

My solution to these problems is as follows:- Two copies of the computer contents are taken at the earliest opportunity during an investigation, and preferably in the presence of the owner (or his legal representative). When the copies are completed the owner is invited to choose one of them to be sealed in his presence. This sealed copy is signed by the owner or his legal representative and is then kept secure by the police. Forensic examination is conducted on the other copy and the computer is returned to the owner.

In the event of a challenge to the integrity of the working copy, the court can order the seal to be broken on the secure copy and this can be verified - if necessary by independent examination.

The security of this process would be greatly improved if some system of internal verification were implemented within the copying procedure such that any subsequent alterations might be located and identified.

If the computer is to be seized and not returned, only a single copy is necessary for working purposes since the seized computer will constitute the 'best evidence'. However, even in these cases and given the transient nature of some of the storage systems (notably within volatile storage on hand held computers) perhaps an additional sealed copy would be seen as a desirable safeguard.

While this represents a relatively simple solution to a difficult problem, it should not be applied too liberally since it leaves the possibility that criminally significant material might be left in the hands of the computer owner. Where there is doubt, it would be better to temporarily seize and seal the computer until the presence or absence of criminally significant material could be positively established.

In Conclusion

Within the published Codes of Practice (HMSO, 1995) concerning the Police and Criminal Evidence Act 1984 (s.60(1)(a) and s.66), section B.6.5 states:- *"Where an officer considers that a computer may contain information which could be used in evidence, he may require the information to be produced in a form which can be taken away and in which it is visible and legible."* I suggest that a forensically sound copying process fulfils this requirement perfectly.

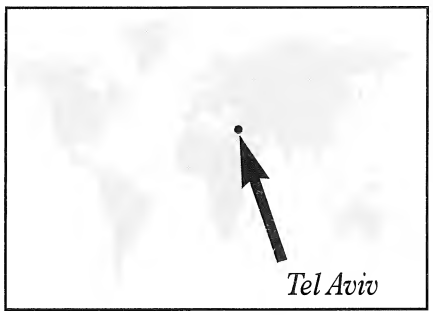
Section 69 of the Police and Criminal Evidence Act 1984 requires that:- *"...at all material times the computer was working properly..."* I suggest that a forensically sound copying process would automatically confirm this *at the time that the evidence is gathered* and thus free the courts to decide upon the validity and applicability of the evidence rather than its integrity. Note that if the copying process uses its own processor, this too must be certified as 'working properly'. Testimony concerning the operation of the computer during the creation or storage of the evidence would then become a completely separate issue.

However, section B.6.7 of the Codes of Practice further states:- *"Property shall not be retained ...for use as evidence or for the purposes of investigation ... if a photograph or copy would suffice for those purposes."* It will be seen from my comments above that strict adherence to this principle might place an investigating officer in the position of allowing a crime to continue (e.g. possession of pornographic material). This is obviously an area which requires urgent review. ■

by Jim Bates, *BSc (Eng), FIAP (Cmpn), President of the Institution of Analysts and Programmers, UK.*

Israel

Computer Forensics the Hard Way



Increasing workloads are not a new phenomenon - but how many forensic investigators need to speak, write and investigate crimes using multiple languages, and all this whilst under a constant awareness of possible terrorist action. The threat of a strategically placed bomb inside the casing of a computer, which could precipitate the next phase in an ongoing war, is an ever present and additional stress factor for Israel's busy computer forensic squad.

Gary Littwin, US born, but now resident in Tel Aviv, is head of the four man computer forensic team who deal with all aspects of computer investigation for the Israeli police force. Using primarily Pentium based computers and custom written forensic software, they are undoubtedly some of the most clued up forensic investigators in the world. The team, Gary Littwin, Eran Safra, Meir Zohar and Isik Kasiel, are based in Tel Aviv on Israel's Mediterranean coast, and working from their office at Police Headquarters, have the same countrywide jurisdiction accorded to all Israeli police officers.

Israel's multilingual and multicultural society lives in a country which is only 450 kms from North to South and, on average, 60 kms from East to West. It is bordered by Lebanon, Syria, Jordan and Egypt with its western shoreline being the Mediterranean Sea.

With such close proximity to so many diverse cultures and nationalities, it is no surprise to discover that Hebrew, Arabic, English, Russian and Amharic (Ethiopian) are all widely spoken by the residents of Israel as their first language. This presents its own problems when investigating a computer crime; to address this, Israeli investigators need to be proficient in several languages, as they deal with suspects and software from all over the world.

Added to the language difficulty there is the localised need to work in four different alphabets and numeric systems. Cyrillic, conventional western alphanumeric, but primarily Hebrew and Arabic are all part of the task faced by the Israeli team. Much of the specialised forensic software used for making data searches in these languages is written 'in house' by forensic investigators Meir Zohar and Eran Safra. One of Zohar's first tasks was to write software to enable the unit to make mirror images of suspect hard disks. This enables an investigator to connect a forensic workstation to the parallel port of a suspect's computer and copy the target disk onto a hard drive in the workstation. The software creates a mirror image of the target drive whilst leaving evidence untouched.

Zohar's innovative work on investigative software has also made the task of trawling through and identifying suspect data far less troublesome. He has created a software program 'Disk to File' which has the capability of changing the whole contents of a seized computer's hard drive into a single, enormous, ASCII file, which can then be searched for key text using conventional forensic examination software. To recover the data converted by 'Disk to File', Zohar has created another piece of software which enables the reconstruction of a suspect's disk from the single ASCII file. This, somewhat understandably, is called 'File to Disk'. ASCII codes for Hebrew characters in Windows are not like those found in DOS documents. This has presented the forensic investigation team with some hefty challenges when converting disk contents into a uniformly searchable file.

Zohar has recently created a package which takes any form of Windows text file, written in any language, and by adding suitable screen font data, converts the character set into a DOS readable ASCII file. Zohar said: "We are very happy to pass this information to other investigators around the world as it will almost certainly make their lives easier. A police force, outside Israel, uncovering data written in a foreign language could find this program very useful."

Hebrew is written from right to left, and so is Arabic. The problems associated with working from right to left in a key word search using conventional western forensic software gave the team some trouble - but this seems to be resolved - they now enter the key words back to front!

Education of all kinds is given a very high priority in Israel; this is extended to the police in the form of lectures and courses which are aimed at increasing awareness of computer forensic procedures.

Littwin said: "A part of our job involves lecturing on forensic computing to the rest of the police force in order to raise the profile of the work we are doing - we hope this will encourage police officers to learn more about the way we handle electronic evidence."

All four investigators create and teach courses in computer crime prevention and investigation. The revenue from these courses give the unit an element of financial independence, and it is the unit's intention that they should become financially self-supporting in the near future.

They face the same difficulties experienced by many computer based units when those holding the purse strings don't understand the technology involved and cannot understand the speed at which investigation equipment becomes obsolete.

Littwin said: "Financial independence will remove the need to explain why an ever increasing equipment budget is needed."

The computer forensic unit also serve as advisors to other police units. They are consulted regularly on matters pertaining to computer crime of all kinds, and a large part of their task is liaison with less experienced police units.

Presenting electronic evidence in Israeli law courts is much the same as in any other country in the world. The court demands positive proof, and both prosecution and defence lawyers are becoming highly computer aware.

The main difference between Israel and much of the Western world is the absence of a jury system. In important cases three judges sit and consider the evidence brought in front of them. They make the decisions and forensic evidence has to be presented to them.

Under Israeli law, a seized computer can only be held for 48 hours before it has to be returned to the owner unless, of course, the computer is found to be holding evidence that pertains to a crime.

If evidence, or an indication that evidence is present on the computer, is discovered then the investigating officers can apply to the court for an extension of the time limit to allow for more intensive or thorough searches.

The 48 hour law was established to prevent the police from holding on to a computer for unnecessarily long periods of time, thereby damaging the owner's business. This protection for the public was seen as vital to the economic growth of a relatively new nation but is now being seen by many as needing change.

Littwin said: "There are moves afoot to change the law to make the time limit longer or even to abolish it entirely. An alternative is to have mirror disk images made acceptable to the justice system, but all this takes time, and the problems don't get any smaller while we wait."

This sort of legal imperative does put a lot of pressure on the forensic team to produce evidence quickly, and some of their methods and software tools have been especially developed to allow fast and accurate investigation of suspect hard drives and electronic media.

Whilst the law was established for the best of reasons, it still makes a lot of work for the investigative team. They need to work around the clock to investigate suspect machines and feel that their resources are sometimes stretched to the limits when a large investigation is underway. They are looking to add members to their team, but have the greatest difficulty in finding technicians of the calibre needed.

Part of the daily task of the Israeli forensic investigation unit is to address the problems related to telephone and communications crime. They are seen by the whole Israeli police force as the main source of communications data. Isik Kasiel was, however, quick to point out that there are specialist agencies in the security forces who deal with matters of national security, and the police deal with the large scale incidence of international phone crime.

The problems range from relatively straightforward exchange cracking and telephone system manipulation, to international sex lines and abuse of the Freephone system. The problem is escalating and will continue to do so as the number of people who become computer literate rises. Israel currently has one of the highest levels, pro-rata, of computer literate citizens. The number of PCs per head of population is also believed to be amongst the largest in the world.

Specialist Communications Investigator, Eran Safra said: "Children as young as twelve years of age are being used to crack the codes which allow access to digital communications networks. They then pass the information over to others who use the phone service to make international calls for free. We also have a problem with free answerphone services being hacked, and then sold for less than the telephone company's charges. These are sometimes used as international sex lines and are very difficult to track."

Hacking data is frequently displayed through local Israeli BBS (Electronic Bulletin Boards). Hackers simply log into the BBS to get the latest hacks, and to upload their own contributions.

The upsurge in mobile computing has brought its own problems - it is not uncommon for the police force to seize laptop computers during the course of other raids. These have recently been used to hold details ▶

of drug operations, and also files pertaining to the lucrative trade in forged identity papers. Scanned images of genuine papers are used to create high quality forgeries which, given Israel's strict immigration policy, are sold for substantial sums on the black market.

There is no doubt that terrorist activity has links to computing, but almost all of this is dealt with by specialist Israeli government security forces. The threat, however, is always present and the unit are always aware that they could seize a booby trapped computer. They offer a few words of advice to those who find themselves in this situation:

- Never simply turn on a machine without checking inside first.
- Never open a computer case without first making a thorough external examination.
- Always check the cabling and components thoroughly.
- Always identify any unusual or unknown parts of a system.
- Remember that ½ kilo of Semtex can be packaged to look very much like ½ kilo of heroin, and removal from the computer's chassis for positive identification could cause a detonation.
- But, perhaps the most important point to take on board is that all computer systems even suspected of containing explosives should be dealt with by a bomb disposal squad.

Littwin said: "We are very happy to share our expertise with police forces in other countries and hope that some will see their way to sharing information with us - there is no point in re-inventing the wheel in every country. We see the exchange of software tools and specialist forensic data as the fastest way to crack down on international criminals." ■

by Ray Hatley

Concealed Evidence

During the investigation of a recent extortion case officers from West Mercia Constabulary seized a personal computer, and quantity of floppy disks, which they believed to contain incriminating information. Back at base the items were copied and the copies carefully examined. However, despite detailed analysis, there was no sign of the expected evidence.

Convinced that there must be evidence somewhere, possibly on a second hard disk, the officers removed the cover. There was no other hard disk present but taped inside the cover there was a floppy disk. On examination this proved to contain vital and incriminating evidence. The case is proceeding. ■

Technical Tip

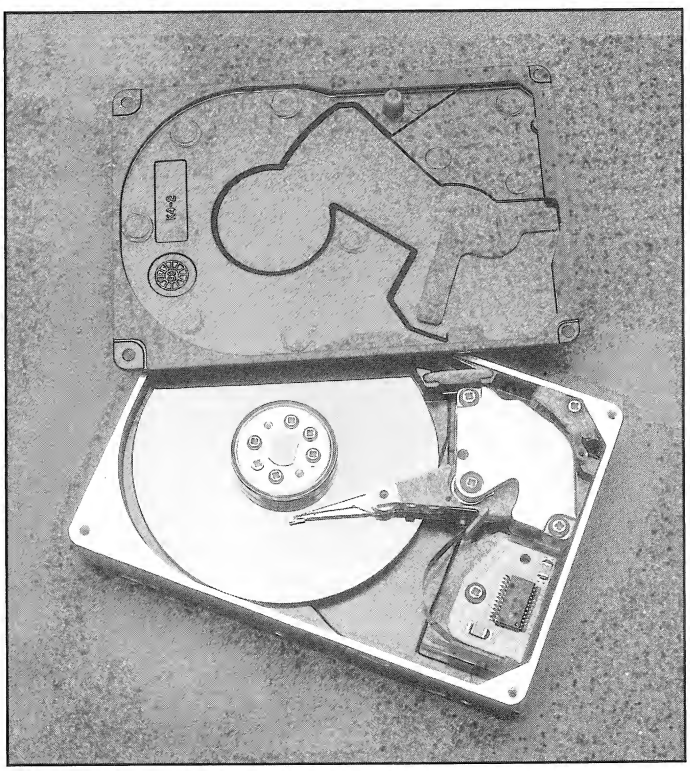
This month's tip comes from Isik Kasiel (Israeli Police)

Make sure disk sizes are shown accurately on diagnostic software and in the BIOS. It is very simple to change the settings in the computer's BIOS to make a large disk drive look considerably smaller, this can be reflected in diagnostic software results which use the BIOS to obtain their data.

It is possible to create a secret partition on a hard drive which can be very tricky to detect. An investigator making a cursory examination could easily overlook the additional partition.

By creating an additional 100Mb partition, a 600Mb hard drive can be made to look like a 500Mb hard drive. This is made more complicated to detect if in the BIOS settings the disk is set up as a 500Mb hard drive. The BIOS will read 500Mb although the actual disk size is 100Mb larger.

To be sure of the real size of a suspect hard disk, run auto-detect from the BIOS which will give the true disk size regardless of partition settings. ■



Case Study

Blackmail

This article describes an actual investigation into alleged blackmail where the evidence was solely derived from computer stored material. Some of the details have been simplified to allow a clearer illustration of the principles involved.

Background

The police in the UK received a complaint from a Mr. C, alleging that he was being blackmailed. The evidence was in the form of a floppy disk on which was a word processor data file which contained a number of allegations, threats and demands. The floppy disk was known to have been sent by a Mr. A, a computer consultant and friend of Mr. C. It was explained that letters were often exchanged on floppy disk in this manner. Police officers immediately went to interview Mr. A and found that he was on holiday abroad. However, his business premises were open and a computer found there was seized for examination.

Preliminary investigation found a letter similar to that on the floppy disk but without the threats or demands that made it actionable. No other relevant files were noted.

When Mr. A returned from holiday he was interviewed, and admitted sending the floppy disk. He admitted writing the letter found on his own machine but denied making the threats and demands. He suggested that Mr. C had added these himself in order to discredit Mr. A, and thus avoid payment of an outstanding invoice for work undertaken. When the interviewing officer indicated that a more detailed investigation of his computer was being prepared, Mr. A offered his full co-operation but suggested that care should be taken in the investigation since during his absence on holiday, his computer was available for Mr. C to use. It was therefore possible that Mr. C had used the computer to introduce the threats and demands into the file on the floppy disk and this may have left traces which might be misinterpreted as suggesting that Mr. A had made them.

The Forensic Examination

A forensic examination was conducted on the contents of the computer hard disk and this revealed a total of 17 recognisable fragments of the letter located in various areas of disk space. One of these was the 'clean' letter noted in the preliminary investigation, the remainder were traces which remained after processing or deletion of the relevant files.

To understand how the examination was conducted it is necessary to describe some of the basic principles of computer operation when textual documents are processed and stored.

Storage space on a disk drive is allocated as required in blocks of a specific size, these blocks are known as clusters. The size of each cluster may vary between computers but is fixed on a single machine. The machine in this case had a cluster size of 16,384 bytes.

As information is stored it is written to the currently allocated cluster (overwriting any existing information) until no more space is available in that cluster, whereupon an additional cluster is allocated and processing can continue. When a file is deleted, the clusters are de-allocated so that they may be re-used elsewhere *but the contents of each cluster are not normally erased.* Thus it will be seen that traces of file contents may remain in their original locations until the relevant clusters are reallocated and overwritten. Information may thus be found in clusters currently allocated to files, clusters currently unallocated and clusters which, though allocated to new files, have only been partially overwritten.

Figure 1 illustrates three of the primary areas where information may be found and they are categorised as Active Space (currently allocated and in use), Inactive Space (currently unallocated and available) and Slack Space (currently allocated but as yet unused by the owning file). ▶

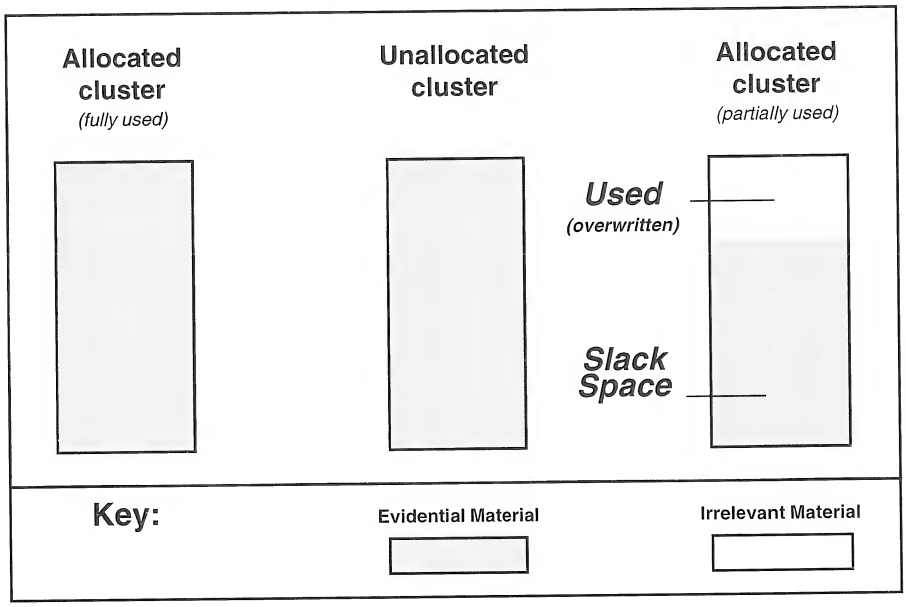


Figure 1: Storage Space Classification

It is also useful to have some idea of exactly how much textual information may be contained in each cluster. Early computers tended to standardise printed output to a page of 80 characters per line and 66 lines per page. This gives 5,280 characters per page.

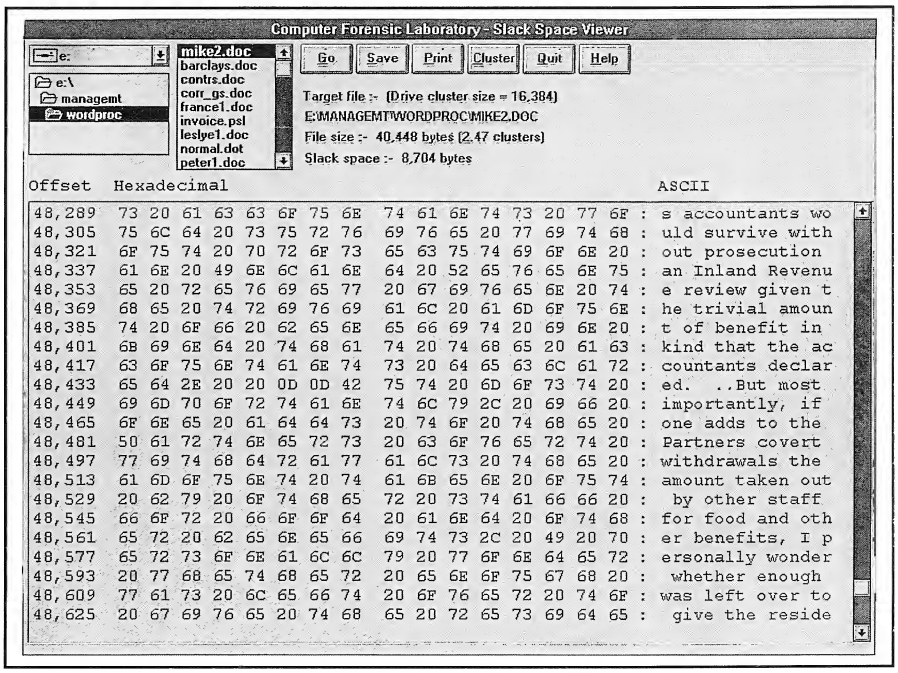
Later developments introduce variations in typeface size and line spacing but this amount is still a useful rule of thumb. Thus since each byte may contain a single character, a single cluster of 16,384 bytes may contain slightly over three pages of textual information. In this case, the original letter was just over 7 pages long and took up fractionally more than two clusters on the floppy disk.

It should be noted that the textual content was preceded in the disk files by technical layout information used by the word processing software and this meant that text information invariably appeared in the latter portion of the file.

Result of the Forensic Examination

The 17 recovered fragments varied between 9,000 and 33,000 bytes in length (2 pages to the whole letter). One was in Active Space (the 'clean' letter), fifteen were in Inactive Space and one was in the Slack Space of another file. The textual content of each fragment was printed out and the fragments were compared. This enabled the fragments to be placed in a unique sequence indicating precisely how the original document had been written and subsequently edited through a number of subsequent revisions.

The sequence showed that the document had originally contained most of the actionable threats and demands. As the sequence progressed, the content changed until the point (midway through the sequence) where the 'clean' letter was produced. The sequence continued with the re-inclusion of the threats and demands but in a slightly different form (for example the amount of money demanded was changed) until the final fragment which matched exactly to the letter produced on the floppy disk. Quite obviously this did not accord with Mr. A's assertion that the letter had started off 'clean'.



Such dates as were available within the computer filing system indicated that the processing had taken place before Mr. A went on holiday, but dates and times on computer files are not conclusive and it was not immediately possible to fix any part of the editing sequence to a particular date that could be independently confirmed. However, the single fragment found within the Slack Space of another file provided a final link to the outside world.

This fragment was located late in the sequence, after the re-introduction of the threats and demands. The cluster containing this fragment had been allocated to another letter unconnected with the case and when police officers interviewed the person to whom the letter had been addressed, he confirmed that he had received it on the day that Mr. A had gone abroad on holiday. This fixed the whole sequence in time and showed Mr. A's story to be completely false. The threats and demands had been re-introduced into the letter at least two days before Mr. A went on holiday - Mr. C could not have been involved.

Mr. A has pleaded guilty to the charge of blackmail but there are many other complicating factors in this case and investigations are continuing. ■

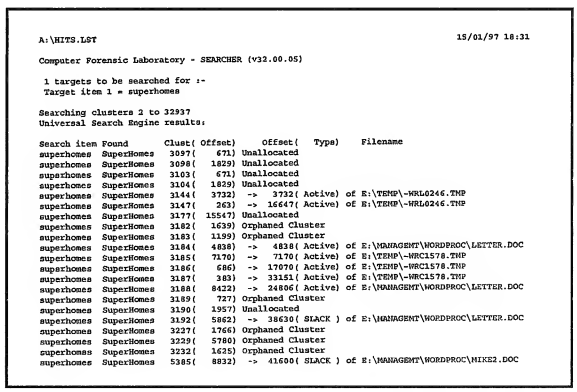


Figure 2 (above):
Screen print of the contents of a letter found in file slack space.

Figure 3 (left):
Print out of the results of the search for 'Superhomes' showing the location of 'Hits'

Book Review

Computer Evidence:

A Forensic Investigations Handbook

by Edward Wilding.

Sweet & Maxwell Ltd., 100 Avenue Road, London NW3 3PS.

236pp. £39.00 sterling. ISBN: 0-421-57990-0

Fraud, forgery, data manipulation, extortion, sabotage and electronic impersonation investigation are only a small part of this new book from Edward Wilding.

Wilding's book sets out to offer expert and well written commentary on the latest in high tech crime techniques, and then to establish ways in which the application of computer forensics may be used to combat them. It is that rare thing, a book for technical people by a technical expert, written in a way which makes it enjoyable to read.

Key features include explanations of the investigative methodology employed to identify network abuse, detailed information on examining personal computers, an excellent collection of glossaries, lists of diagnostic software and a directory of consultants and agencies useful to the computer investigator.

Computer Evidence is a very positive book which explains in simple terms, using excellent case studies, exactly what computer forensics is all about. It is written by a man who obviously knows his subject, and delights in explaining it.

Wilding is a leading figure in the world of computer forensics, and his book reflects years of practical experience in this field. His guidance in the complex field of electronic forensic evidence presentation will be invaluable to novice and expert alike. The newcomer to forensic computing will, additionally, find a wealth of technical detail and procedural advice in this book, whilst the case studies will be of immense interest to the more experienced investigator. Highly recommended. ■

Profile

Paul Sullivan

Paul Sullivan, based in Sydney, Australia, is currently Director for Business Fraud Risk Services at Arthur Andersen, one of the big six international accountancy firms. His work is mainly involved with investigating computer fraud cases, but he has an active interest in developing preventative measures against all kinds of crime.

Sullivan said: "We have Arthur Andersen investigative teams in most of the major countries in the world giving us an incredible network of people - so if we get a job that starts in Sydney and moves to the US then it is simply a matter of telephoning the States to get that team to take over. It is a kind of commercial Interpol. The need is definitely there for this kind of service."

In his fifteen years as an operational detective, Sullivan has been attached to various sections including the fraud task force group, the major crime squad, and several commissioner task forces. His area of expertise is the investigation of white collar crime and more specifically computer related offences, such as computer fraud, credit card offences, and insurance fraud.

In 1995 Sullivan presented a paper at the first International Conference on Computer Crime at Interpol Headquarters in Lyon, France. He has also undertaken field research in Europe, Asia, the United States and the United Kingdom.

In addition to his remarkable work record with the New South Wales Police, Sullivan is also a respected academic and is currently a Visiting Research Fellow at the New South Wales Police Academy within the School of Investigation and Intelligence.

Sullivan has a Masters Degree in Business with his thesis on computer related crime. He is currently in the 2nd year of a doctorate in philosophy at the University of Newcastle where he is researching the role of the commercial sector in the investigation of computer related crime. He is also a Research Associate for the Australian Computer Abuse Research Bureau at the Royal Melbourne Institute of Technology.

Paul Sullivan specialises in the education of people to stop them committing crimes in the first place. He regards preventative measures as the logical place to start and said: "In the vast majority of Australian fraud cases, offenders are employees of the victim and most are first offenders. There are three major things that cause people to commit crimes, drugs, gambling and lifestyle - with gambling being by far the most common reason why people offend."

Sullivan's advice to industry is straightforward: "Set up a department in the personnel section where people can ask for advice or help when things go wrong for them."

> ***"Giving people an alternative to theft is far better than prosecuting them. Minimise the incidence of workplace crime by instigating effective ongoing screening processes, implementing education procedures and, most importantly, creating a 'whistle blower' programme. The most effective tool is a confidential service where people can report offenders without fear of repercussions."*** ■

Who Commits Computer Crime

In our high tech world where we struggle to ensure computer system integrity and security, it is easy to gloss over the fact that all crime is committed by real live people.

So what sort of people do commit computer crime, and are there any distinguishing characteristics which may help an inexperienced investigator spot the villain amongst the innocents?

The Computer Crime Adversarial Matrix, first developed for the FBI, would have us believe that there are three distinct categories of offender: Criminals, Hackers and Vandals. The three categories overlap substantially and are probably best viewed as classifications subject to individual motivation. The primary motivation of a criminal is gain, the hacker will look to achieve illicit access and the vandal seeks to destroy or damage.

The concept of stereotyped criminals is, obviously, rather foolish - but it may be possible to identify some of the common behavioural or personality traits which cause a person involved in computer crime to act in a certain way.

Vandals are frequently angry people, in a job they do not enjoy, who see an opportunity to 'get even' with the owner of the target computer. They are often quite ineffectual people who would not consider damaging computer equipment in a physical sense, but have no qualms about wiping files, scrambling data and planting logic bombs.

Vandals may also see the opportunity to benefit financially from their actions and few can resist the urge to do so. This, however, is rarely the primary motive behind computer vandalism.

Hackers are often attracted to hacking by the intellectual challenge it presents - they are frequently bored and have a lot of time on their hands. They often hack at night because they have to work during the day at menial, often low paid, jobs or attend school or college.

Hackers are usually highly intelligent, and regard hacking as a form of revenge on an unappreciative society. They frequently regard their actions as demonstrations of intellectual superiority.

Computer hackers often have international connections via the Internet, they use e-mail and international bulletin boards to exchange information on target systems, but have no real organisation.

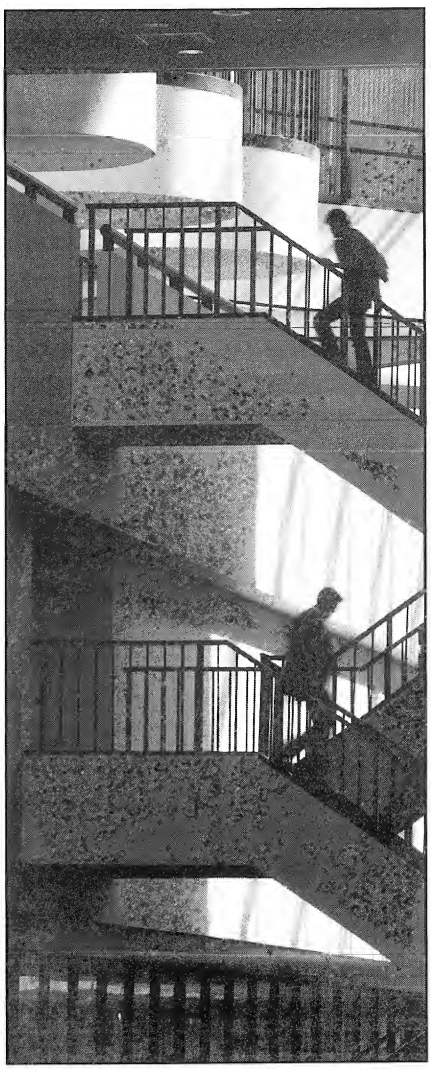
Hackers, or as they are sometimes referred to Crackers, are frequently involved in what has become known as phone phreaking; the fraudulent use of telephone company resources.

Because of their commonly low financial status, phone phreaking is often the only way hackers can access computers in other parts of the world. They often see computers in other countries as more legitimate targets and feel safer because they are geographically removed from the scene of the crime.

In the main part, hackers do not see their actions as being those of a criminal. Some regard themselves as computerised heroes who point out the weaknesses in corporate systems, but this argument is made irrelevant when they then demand a ransom for divulging their modus operandi. Hacking is virtually encouraged by those corporations who pay the hacker's ransom so that they can prevent further system invasion by added security measures. The hacker is further aided by the general reluctance of industry to admit to an attack.

Criminals can be divided into two groups - those who steal by fraudulent use of computers or by any sort of computer system abuse and those who take part in corporate espionage.

The fraudsters have created a growth industry - from large scale organised crime involved in the laundering of drug money, to the actions of smaller organisations and individuals who see computer fraud as an easy and safer way of making large sums than robbing banks. ▶



Seizing & Storing

Individuals are often the hardest to detect. They do not share their information but, like many criminals, are caught when they become sloppy in their methods or greedy. They frequently give themselves away by marked changes in their lifestyle.

Espionage is usually undertaken by highly skilled operatives with massive governmental or corporate resources. Agents are usually fully aware of the measures in effect to thwart their activities and make full use of their financial power to pay for information or to pay others to do the high risk part of their operations. Hackers are often recruited to break into a system and deliver access codes to their controller.

A technique known as social engineering has become common, where an employee is approached - often on an internal phone system - and sensitive information requested with the assurance that the recipient is also an employee of the organisation so the information is 'safe'. This information, often in the form of passwords or system data, is then used to gain access to restricted parts of a system or even, in the case of software development companies, to sensitive source codes.

Social engineers are a very specific type of computer criminal. They rely on goodwill and an ingenuous personality to extract their information and are, perhaps, the most difficult criminal to identify. Crimes involving social engineering are frequently not exposed because their victims feel foolish and do not want others to know of their gullibility.

More detailed information is available on the types of people involved in computer crime, and the above is only a short precis of the problem. The fact remains that obtaining proof of criminal activity is the only sure way of identifying a perpetrator. ■

by **Ray Hatley**

An article in Issue 1 has prompted some readers to contact us in connection with the seizure and storage of suspect equipment. The following are guidelines which may act as a starting point from which departments may develop their own strategy to seize and store computers.

In all search and seizure operations it is vital that the investigator adheres to procedures which will preserve evidential continuity and integrity.

On seizure

Note the layout of the equipment, particularly the connection of all cables. Clearly mark each cable plug and corresponding socket. If required, the equipment may be reassembled at a later date. Note the make, model number and manufacturer's serial number. Clearly number each piece of equipment. Ideally at this stage, photographs should be taken.

Place each CPU in a stout clear polythene bag and close with a numbered plastic seal. Make a note of the seal number. In some climatic conditions, it may be advisable to have small holes punched in the bag which will help to prevent possible condensation.

Floppy disks and other storage media also should be placed into polythene bags. Each bag should be closed with a numbered plastic seal and the seal number noted. Each seized item should be placed into its own evidence bag. For example, all floppy disks found next to the computer on top of the desk should be placed in one bag; those found perhaps in a box in a hall cupboard should be placed in a new bag. The location of each item should be clearly marked on the bag label or a control sheet. Information about the location in which the disks were found may prove useful during the subsequent forensic examination.

Although it may be said that it is not essential to seal monitors, keyboards, connectors and other non-storage materials, it is advisable to do so. This will help to prevent any possible subsequent damage, or even loss.

On copying / examination

Normally only the CPU and any other storage media (floppy disks, optical cartridges, CD ROMs etc) are required for copying. Any standard monitor and keyboard can be connected. However, for those few exceptions which require dedicated equipment, the original seized items should be readily available.

Prior to examination of each sealed item, a worksheet should be completed with basic details about the equipment. This should also record the original seal number. The seal should then be cut, the equipment to be examined removed from the bag, and the cut seal placed in the bag.

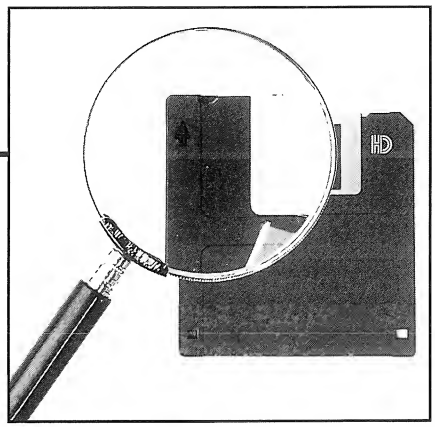
During copying / examination, whilst unsealed, the equipment should be kept in a secure place. If left unattended in a non-secure location, the equipment should be resealed in the evidence bag and the seal number noted. When the second (and any subsequent) seal is cut this should also be placed in the evidence bag.

On completion of copying, the item should be returned to the evidence bag which should contain the original cut seals. The bag should be resealed with a new seal and the number noted on the worksheet together with details of the examination undertaken.

Long-term storage

All items should be kept in stout polythene evidence bags and sealed as detailed above. The storage area should be dry, dust free, and of an even temperature. Items should not be placed near central heating pipes, in direct sunlight or near sources of magnetic radiation. ■

Forensic Q&A



Q *I've been told that if I want to look at the contents of a seized computer I should never just switch it on. Why is this and what should I do?*

A When a computer is switched on instructions are successively loaded into memory by the processor. The first instructions are those which detail the physical characteristics and functioning of the hardware, such as the type of hard disk, amount of memory and speed of processor. The next level of instruction is that which deals with the storage, retrieval and general manipulation of both data and program files. This is called the operating system and is normally located on the hard disk. Once the operating system has loaded successfully, further instructions may be executed to load graphical user interfaces and applications such as word processors and spreadsheets.

During the loading process, which is referred to as 'booting', some programs may execute sets of instructions which write data and/or log files back to the computer's hard disk. If this occurs there are two major problems from a computer forensic's viewpoint. Firstly the integrity of the evidence will be compromised because the hard disk contents have been altered since the computer was seized. Secondly when the files are written to the hard disk they may be located in areas that were previously occupied by information that may be pertinent to the investigation, e.g. deleted files. Such overwritten information is permanently lost.

The way to avoid this problem is to switch on the computer using a floppy disk located in the A: drive and containing the operating system, referred to as a boot disk. The information on the hard disk should then be copied onto another medium prior to further examination. It is essential that any copying is undertaken with software which is known to prevent information being written to the hard disk and, preferably, which has been specifically written for forensic work.

Q *During a raid I have recovered a plastic box containing a cartridge that looks like some sort of computer disk. On the box is written SyQuest. What is this and how can I access it so that evidential integrity is preserved?*

A The SyQuest is a type of removable hard disk which was designed to fit into a compatible 5.25inch drive. The earliest version had a capacity of 44Mb, which was later increased to 88Mb. More recently a 3.5inch version was produced which is still available, the latest version having a storage capacity of 230Mb. At the time it was produced, the SyQuest was an efficient and cost effective means of data storage and many were manufactured. It is still in use, especially for backup and archive purposes.

A SyQuest drive is connected to a PC (or an Apple Mac) using a SCSI adaptor and for forensic examination purposes can be treated as a normal hard disk. It can be copied using any of the proprietary copying software, and the information analysed as usual. If a SyQuest cartridge is recovered without the machine in which it was used, the main problem will be finding a suitable drive with which it can be read (particularly the older 5.25inch drives which are no longer available from suppliers). Unless a large number of cartridges are involved it may be more practical to have the material copied to current media by a sub-contract computer forensic service.

Q *How would I proceed if I went on a raid where a network was in place rather than stand-alone PCs?*

A There are many different types of network, some simple to access and copy, others requiring specialist technical knowledge. With the former, regardless of size, each machine can be copied separately, including any file servers. The more complex network will require a forensic strategy based on the specific configuration of hardware and software found.

Prior to any raid involving computers try to get as much information as possible about the type of equipment involved. If you know you will be faced with a complex network ensure that you will have the appropriate specialist advice and assistance. If you cannot ascertain the type of equipment in advance, make sure that you will have access to specialist advice should you need it.

It is important to remember that copying the network will be the simple part of the exercise. Accessing the copies and performing the analysis in a correct and efficient manner will be much more difficult. ■

Please address your questions and / or comments to:
Forensic Q&A
IJFC, Third Floor, Colonnade House
High Street, Worthing, West Sussex
UK BN11 1NZ
e-mail: ijfc@pavilion.co.uk

Readers are advised to seek independent specialist advice before commencing an investigation.

Notice Board

We will be pleased to receive contributions to this page. Please mark all correspondence 'Notice Board'. We reserve the right to edit if required.

EVENTS

Computer Forensics: Computer Evidence and the Law

11 March, Uxbridge, UK

This lecture, which has been organised by London West branch of The British Computer Society, will be held at Brunel University, Lecture Centre, Theatre B, 7.30pm.

Contact: Mr A Dransfield
Tel: +44(0)171 637 9111

19th Annual Colloquium on Information Retrieval Research

8-9 April, Aberdeen, Scotland

The Robert Gordon University in Aberdeen, will provide a forum for IR researchers to disseminate their work and an opportunity to learn more of research in progress.

For more information see:
http://www.scms.rgu.ac.uk/bcs-irsg97/home.html
Contact: Jonathan Furner PhD,
The Robert Gordon University
Tel: +44 (0)1224 283835
Fax: +44 (0)1224 492608
e-mail: j.furner@rgu.ac.uk

Computer Forensics: Computer Evidence and the Law

17 April, Cheltenham, UK

Another opportunity to hear this lecture, this time outside London. Organised by The British Computer Society, to be held at the Teaching Centre, Park Campus, Cheltenham and Gloucester College.

Contact: Mr R Jardine
Tel: +44(0)1242 221311

The second international seminar on advancing the scientific investigation of crime

6-18 July, Durham, UK

The seminar will be of interest to senior police officers who have responsibility for the scientific investigation of crime, forensic scientists, crime scene examiners and those responsible for training in the field of scientific support to crime investigation. The programme will include visits to the National Training Centre for Scientific Support to Crime Investigation and to the Laboratories of the Forensic Science Service.

Contact: The British Council
Tel: +44 (0)1865 316636
Fax: +44 (0)1865 557368

TRAINING

The Centre for Research in Computer Related Crime

Training Programme for 1997 is currently in preparation. If you would like to be placed on their mailing list to receive details, please send your name and address to:

CRCRC Short Courses Organiser,
Computing Services, Queen Mary and Westfield College, London E1 4NS.
Tel: +44 (0)171 975 5295
e-mail: crcrc@qmw.ac.uk

Please contact the Centre if you would like specific topics covered.

Training in Computer Forensics

Four modules comprising:
Fundamental Computer Forensics
Applied Computer Forensics
Advanced Computer Forensics
Legal and Procedural Computer Forensics
Courses held monthly in West Sussex.

Contact: Computer Forensics Ltd
Tel: +44(0)1903 823181
Fax: +44(0)1903 233545

NEWS

The British Standards Institute has issued a *Code of Practice for Legal Admissibility of Information Stored on Electronic Management Systems*. This Code of Practice deals in depth with issues of legal admissibility, authenticity, and evidential weight of information concerning documents stored in electronic systems on write once optical media (WORMs). Specifically excluded are systems using re-writable media since these are considered to require much more stringent control.

The Code reference is DISC PD0008, price £19.50, and it is available from:

The British Standards Institute,
389 Chiswick High Road, London W4 4A1.
Tel: +44 (0)181 996 9000

Cayman Islands lead fight against offshore financial crime

A major international Commercial Crime Prevention Conference took place in the Cayman Islands in January. It focused on information sharing about money laundering, fraud and other financial crimes with the aim of increasing awareness and developing further measures to combat these problems. The conference was attended by an international audience comprising diplomats, civil servants, parliamentarians and representatives from the business and finance sectors.

For further information contact Miranda Pugh at the Cayman Islands Government Press Office. Tel: +44 (0)171 976 8263
Fax: +44 (0)171 222 2030

Worldwide software piracy losses are estimated at $13.1 billion.

The results of the first independent survey on global software piracy estimates have been released by the Business Software Alliance (BSA) and the Software Publishers Association (SPA). The survey evaluated sales data and market information for 80 countries, and was based on 27 business applications. The software piracy losses of $13.1 billion estimated for 1995 show a 9 percent increase over the $12.2 billion estimate for 1994. Individual country piracy rates and retail revenue loss can be obtained from BSA or SPA.

Contact:
Robin Burton, Legal Affairs Committee,
BSA at Ketchum Public Relations plc,
London. Tel: +44 (0)171 379 3404
Mr Gerard Gabella, SPA Europe
Tel: +33 1 53 77 6377
Diane Smiroldo, BSA, US.
Tel: (202) 530 5136
David Phelps, SPA, US.
Tel: (202) 452 1600

International Journal of FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd.